Dear Parents and Caregivers,

At Immaculate Heart of Mary School we have many opportunities to use Information and Communication Technology to further develop our students’ learning. We have a network of computers across our Resource Centre, our computer room and in the classrooms. Students have access to information through a variety of means – from iPads to information stored on the School Network; as well as the Internet.

The measures to promote cyber-safety of Immaculate Heart of Mary are based on our core values of Love, Hope, Justice, Connectedness and Inclusivity. To assist us to enhance learning through the safe use of information and communication technologies (ICTs), we are now asking you to read this document and sign the attached Use Agreement Form.

Rigorous cyber-safety practices are in place, which include cyber-safety ‘Use Agreements’ for staff and students, who were involved in the development of the agreement. Child protection education, such as the Keeping Safe Child Protection Curriculum and our school based social and emotional learning program, include information about remaining safe when using new technologies and is provided to all students.

The computer network, Internet access facilities, computers and other ICT equipment/devices bring great benefits to the teaching and learning programs at Immaculate Heart of Mary, and to the effective operation of the school. The ICT equipment is for educational purposes appropriate to our school, whether it is used on or off the site.

The overall goal of Immaculate Heart of Mary is to create and maintain a cyber-safety culture that is in keeping with our values and with legislative and professional obligations. The ‘Use Agreement’ includes information about your obligations, responsibilities and the nature of possible consequences associated with cyber-safety breaches that undermine the safety of the school environment.

All students will be issued with a ‘Use Agreement’ and once signed consent has been returned to school, students will be able to use the school ICT equipment. Material sent and received using the school network may be monitored and filtering and/or monitoring software may be used to restrict access to certain sites and data, including e-mail.

Where a student is suspected of an electronic crime, this will be reported to the South Australia Police. Where a personal electronic device such as a mobile phone is used to capture images of a crime, such as an assault, the device will be confiscated and handed to the police.

While every reasonable effort is made by schools and the Catholic Education SA(CESA) administrators to prevent children’s exposure to inappropriate content when using CESA’s online services, it is not possible to completely eliminate the risk of such exposure. In particular, CESA cannot filter Internet content accessed by your child from home, from other locations away from school or on mobile devices owned by your child. CESA recommends the use of appropriate Internet filtering software.


Please do not hesitate to contact me if you have any concerns about your child’s safety in using the Internet and ICT equipment/devices.

Kind regards,

Pauline Kinsman
PRINCIPAL
STRATEGIES TO HELP KEEP IMMACULATE HEART OF MARY STUDENTS CYBER-SAFE

Important Terms:

‘Cyber-safety’ refers to the safe use of the Internet and ICT equipment/devices, including mobile phones.

‘Cyber bullying’ is bullying which uses e-technology as a means of victimising others. It is the use of an Internet service or mobile technologies - such as e-mail, chat room discussion groups, instant messaging, web pages or SMS (text messaging) - with the intention of harming another person.

‘School ICT’ refers to the school’s computer network, Internet access facilities, computers, and other ICT equipment/devices as outlined below.

‘ICT equipment/devices’ includes computers (such as desktops, laptops, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, iPads, MP3 players), cameras (such as video and digital cameras and webcams), all types of mobile phones, gaming consoles, video and audio players/receivers (such as portable CD and DVD players), and any other, similar, technologies.

‘Inappropriate material’ means material that deals with matters such as sex, cruelty or violence in a manner that is likely to be injurious to children or incompatible with a school environment.

‘E-crime’ occurs when computers or other electronic communication equipment/devices (eg Internet, mobile phones) are used to commit an offence, are targeted in an offence, or act as storage devices in an offence.

Parents/caregivers play a critical role in developing knowledge, understanding and ethics around their child’s safety and safe practices regardless of the time of day. Being cyber-safe is no exception and we invite you to discuss with your child the following strategies, to help them stay safe when using ICT at school and after formal school hours.

1. I will not use school ICT equipment until my parents/caregivers and I have signed my Use Agreement Form and the completed form has been returned to school.

2. I will use the computers and other ICT equipment only for my learning and teacher directed activities.

3. I will not access social networking or gaming sites at school or download any games or music etc onto the school network.

4. I will go online or use the Internet at school only when a teacher gives permission and an adult is present.

5. If I am unsure whether I am allowed to do something involving ICT, I will ask the teacher first.

6. I have my own user name, I will log on only with that user name. I will not allow anyone else to use my name.

7. I will keep my password private.

8. I will not store personal files, including music, games or pictures, on the School Network.
9. I will use the Internet, e-mail, mobile phones or any ICT equipment only for positive purposes, not to be mean, rude or offensive, or to bully, harass, or in any way harm anyone else, or the school itself, even if it is meant as a joke.

10. While at school, I will:

   - attempt to search for things online that I know are acceptable at our school. This would exclude anything that is rude or violent or uses unacceptable language such as swearing
   - report any attempt to get around, or bypass, security, monitoring and filtering that is in place at our school.

11. If I find anything that is mean, rude, unacceptable or upsets me, I will:

   - not show others
   - turn off the screen
   - notify a teacher straight away.

12. Only with written permission from home and the school will I bring any ICT equipment/devices to school. This includes things like mobile phones, iPods, games, cameras, and USB/portable drives.

13. Only with written permission from the teacher will I connect any ICT device to the school network, or run any software (e.g. a USB/portable drive, camera or phone). This includes all wireless/Bluetooth technologies.

14. The school cyber-safety strategies apply to any ICTs brought to school.

15. To ensure my compliance with copyright laws, if I download or copy any files such as music, images, videos, games, or programs and I will acknowledge the owner.

16. I will not put any personal information online, unless a parent or teacher has given permission. Personal identifying information includes any of the following:

   - my full name
   - my address
   - my e-mail address
   - my phone numbers
   - photos of me and/or people close to me.

17. I will respect all school ICTs and will treat all ICT equipment/devices with care. This includes:

   - not intentionally disrupting the smooth running of any school ICT systems
   - not attempting to hack or gain unauthorised access to any system or network
   - following all school cyber-safety strategies, and not joining in if other students choose to be irresponsible with ICTs
   - reporting any breakages/damage to a staff member.

18. If I do not follow cyber-safety practices the school may inform my parents/caregivers and my access to any ICT’s at school may be suspended.

In serious cases, the school may take additional disciplinary action against me. My family may be charged for repair costs. If illegal material or activities are involved or e-crime is suspected, it may be necessary for the school to inform the police and hold securely personal items for potential examination by police. Such actions may occur even if the incident occurs off-site and/or out of school hours.
To the Parent/Caregiver/Legal Guardian:

Please read this page carefully to check that you understand your responsibilities under this agreement. Return the signed Use Agreement to the school.

I understand that Immaculate Heart of Mary will:

- do its best to enhance learning through the safe use of ICTs. This includes working to restrict access to inappropriate, illegal or harmful material on the Internet or on ICT equipment/devices at school or at school-related activities
- work with children and their families to encourage and develop an understanding of the importance of cyber-safety through education designed to complement and support the Use Agreement initiative. This includes providing children with strategies to keep themselves safe in a connected online world
- respond to any breaches in an appropriate manner
- welcome enquiries at any time from parents/caregivers/legal guardians or children about cyber-safety issues.

My responsibilities include:

- discussing the information about cyber-safety with my child and explaining why it is important
- supporting the school's cyber-safety program by emphasising to my child the need to follow the cyber-safety strategies
- contacting the principal or nominee to discuss any questions I may have about cyber-safety and/or this Use Agreement.
CYBER-SAFETY USE AGREEMENT

I have read and understood this Cyber-safety Use Agreement and I am aware of the school’s initiatives to maintain a cyber-safe learning environment.

Name of Child.......................................................... Class .............................................

Signature ........................................................................

Name of Parent/Caregiver/Legal Guardian.................................................................

Signature...................................................................... Date................................................

My Child..........................................................................is able to bring the following ICT devices to school:

(Please circle)
USB/Portable Drive iPod iPad Laptop Camera Mobile phone

Name of Parent/Caregiver/Legal Guardian.................................................................

Signature.................................................................. Date..............................................

PLEASE NOTE

This agreement will remain in force as long as your child is enrolled at this school.

If it becomes necessary to add/amend any information or rule, you will be advised in writing.

PLEASE RETURN THIS SECTION TO SCHOOL. A COPY MAY BE DOWNLOADED FROM THE SCHOOL WEBSITE IF YOU WOULD LIKE A PERSONAL COPY